

# Exact Non-identity check is NQP-complete

Yu Tanaka

*Advanced Materials Laboratories, Sony*

March 4, 2009

## Abstract

We define a problem “exact non-identity check”: Given a classical description of a quantum circuit with an ancilla system, determine whether it is strictly equivalent to the identity or not. We show that this problem is NQP-complete. In a sense of the strict equivalence condition, this problem is different from a QMA-complete problem, non-identity check defined in [1]. As corollaries, it is derived that exact equivalence check is also NQP-complete and that it is hard to minimize quantum resources of a given quantum gate array without changing an implemented unitary operation.

## 1 Introduction

Non-identity check, which is defined and proven to be Quantum Merlin-Arthur (QMA) complete in [1], is the problem of determining whether a given quantum circuit (unitary) is almost equivalent to a complex multiple of the identity with respect to the operator norm. QMA is known to be a quantum analog of NP because it is an extension of the verifier-based definition of NP, in that sense non-identity check is one of the hardest problems based on quantum gate array complexity.

There is another quantum analog of NP, non-deterministic quantum polynomial-time (NQP)[2]. NQP is defined as an extension of the Machine-definition of NP, which is a set of decision problems solvable in polynomial time by a non-deterministic Turing machine. Here, we have a question: is there any NQP-complete problem based on quantum gate array complexity?

In this paper, to answer the question, we propose exact non-identity check which is the problem of determining whether a given classical description of a quantum circuit with an ancilla system is strictly equivalent to a complex multiple of the identity or not, and we prove that exact non-identity check is NQP-complete.

It is important to derive a NQP-complete problem based on quantum gate array complexity for at least two reasons. One is that such problems are less well-known because NQP does not

equal QMA. While two definitions of NP are equivalent, the following relation between QMA and NQP is known to be satisfied[3],

**Lemma 1**

$$NQP = \bigcup_{\delta: \mathbb{Z}^+ \rightarrow (0,1]} QMA(\delta, 0), \quad (1)$$

where  $QMA(\delta, 0)$  is defined as QMA with perfect soundness in preliminary. Lemma 1 suggests that NQP does not equal QMA. We use Lemma 1 to prove the NQP-hardness of exact non-identity check. The other reason is that the NQP-complete problem is useful to analyze quantum gate array complexity. For example, we can show trivially that exact equivalence check is NQP-complete from exact non-identity check, where exact equivalence check is the problem of determining whether two unitary operations implemented by two given classical descriptions are strictly equivalent or not. Further, it is derived to be hard to minimize quantum gate resources of a given quantum gate array without changing the content of the implemented unitary operation.

In this paper, first, we give our notations and definitions in preliminary. Second, we propose exact non-identity check and exact equivalence check, and prove the NQP-completeness of exact non-identity check and exact equivalence check. Further, quantum gates minimization problem is defined and proven to be NQP-hard. Finally, we summarize the exact non-identity check.

## 2 Preliminary

We start with giving several notations and definitions used in this paper. A classical bit string  $x \in \{0,1\}^*$  is regarded as an integer if desired.  $\mathbb{Z}^+$  denotes the set of nonnegative integers.  $\mathcal{B} = \mathbb{C}^2$  denotes one qubit Hilbert space. For any Hilbert space  $\mathcal{H}$ ,  $\mathcal{S}(\mathcal{H})$  denotes the set of density operators over  $\mathcal{H}$ .  $\mathcal{H}_a$  denotes Hilbert space for an ancilla system. Further, we define  $|\bar{0}\rangle := |0 \cdots 0\rangle$  and  $|x_+\rangle := H^{\otimes n} |x\rangle$  for  $x \in \{0,1\}^n$ , where  $H$  is the Hadamard gate.

In order to use a result of Ref.[3], we define  $(\delta, \mu)$ -quantum Merlin-Arthur (QMA). The complexity class QMA or BQNP is a quantum analog of NP and was first defined in Ref.[4].

**Definition 1** (QMA( $\delta, \mu$ ))

Given functions  $\delta, \mu : \mathbb{Z}^+ \rightarrow [0, 1]$ , a language  $L$  is in QMA( $\delta, \mu$ ) if for every classical input  $x \in \{0,1\}^*$  one can efficiently generate a quantum circuit  $U_x$  (“verifier”) consisting of at most  $p(|x|)$  elementary gates for an appropriate polynomial  $p$  such that  $U_x$  acts on the Hilbert space

$$\mathcal{H} := \mathcal{B}^{\otimes n_x} \otimes \mathcal{B}^{\otimes m_x}, \quad (2)$$

where  $n_x, m_x$  grow at most polynomially in  $|x|$ . The first part is the input register and the second

is the ancilla register. Further,  $U_x$  has the properties that

$$(\text{Completeness}) \quad \forall x \in L \exists \rho \in \mathcal{S}(\mathcal{B}^{\otimes n_x}), \text{Tr}[U_x(\rho \otimes |\bar{0}\rangle \langle \bar{0}|)U_x^\dagger P_1] \geq \delta(|x|), \quad (3)$$

$$(\text{Soundness}) \quad \forall x \notin L \forall \rho \in \mathcal{S}(\mathcal{B}^{\otimes n_x}), \text{Tr}[U_x(\rho \otimes |\bar{0}\rangle \langle \bar{0}|)U_x^\dagger P_1] \leq \mu(|x|), \quad (4)$$

where  $P_1$  is the projection corresponding to the measurement “Is the first qubit in state 1?”. A quantum state  $\rho$  is called a proof or a witness.

Note that a proof which is a mixed state does not increase the completeness due to the linearity of the quantum operation and the tracing out operation. Here, QMA with perfect soundness or NQMA[3] is defined.

**Definition 2 (QMA with perfect soundness, NQMA)**

A language  $L$  is in NQMA if there exists a function  $\delta : \mathbb{Z}^+ \rightarrow (0, 1]$  such that  $L$  is in QMA( $\delta, 0$ ).

The complexity class NQP is a quantum analog of NP and was proposed as the class of the problems that are solvable in polynomial time by non-deterministic quantum Turing machines.

**Definition 3 (NQP)**

A language  $L$  is in NQP if and only if there exists a quantum Turing machine  $Q$  and a polynomial  $p$  such that

$$\forall x \in L \iff \Pr[Q \text{ accepts } x \text{ in } p(|x|) \text{ steps}] \neq 0. \quad (5)$$

So far, we can use the result in Ref.[3], Lemma 1, to prove the NQP-hardness of exact non-identity check.

### 3 Exact non-identity check and exact equivalence check

Exact non-identity check is the problem of determining whether a classical description of unitary operation is *strictly equivalent* to identity or not. Non-identity check proposed in Ref.[1] is, however, whether a given quantum circuit is the identity with respect to the operator norm or not. To state exact non-identity check problem precisely, we have to define an implemented unitary operation with an ancilla system.

**Definition 4 (An implemented unitary operation with an ancilla system)**

For every classical input  $x \in \{0, 1\}^*$  one can efficiently generate a quantum circuit  $U_x$  consisting of at most  $p(|x|)$  elementary gates for an appropriate polynomial  $p$  such that  $U_x$  acts on the Hilbert space  $\mathcal{H}_{in} \otimes \mathcal{H}_a := \mathcal{B}^{\otimes n_x} \otimes \mathcal{B}^{\otimes m_x}$ , where  $n_x$  and  $m_x$  grow at most polynomially in  $|x|$ . The quantum circuit  $U_x$  implements a unitary operation  $U$  with an ancilla if  $U_x$  satisfies that

$$\exists |\phi_x\rangle \in \mathcal{H}_a \forall |\psi\rangle \in \mathcal{H}_{in}, U_x(|\psi\rangle \otimes |\bar{0}\rangle) = U|\psi\rangle \otimes |\phi_x\rangle. \quad (6)$$

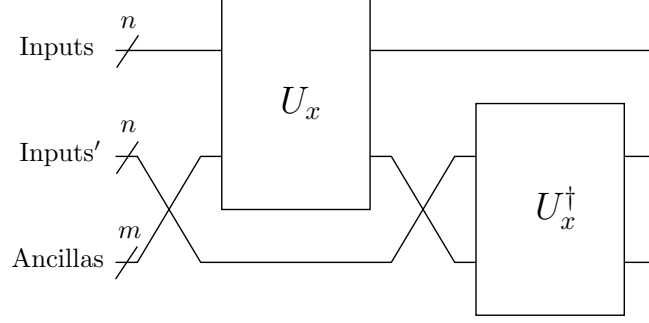


Figure 1: Circuit  $Z_x$  consisting of  $U_x$  and its complex conjugate.

In general,  $|\phi_x\rangle$  is unknown. However, for a quantum circuit  $U_x$  satisfying Eq.(6), we can always take  $|\phi_x\rangle = |\bar{0}\rangle$  by constructing another quantum circuit  $Z_x$  implementing  $U \otimes U^\dagger$  in Fig. 1. In the following, note that for a given classical description of  $U_x$ ,  $Z_x$  denotes the circuit in Fig. 1.

To define exact non-identity check, it is useful to show another equivalent representation of Eq.(6).

**Lemma 2** Eq.(6) is satisfied if and only if

$$\forall |\Psi\rangle \in \mathcal{H}_{in} \otimes \mathcal{H}_{in'}, |\langle \Psi | \otimes \langle \bar{0} | \rangle (U^\dagger \otimes U \otimes I) Z_x(|\Psi\rangle \otimes |\bar{0}\rangle)|^2 = 1. \quad (7)$$

**Proof** Let us show the sufficient condition, since the necessary one is trivial. If Eq.(7) is satisfied,

$$\forall |\psi\rangle \otimes |\psi'\rangle \in \mathcal{H}_{in} \otimes \mathcal{H}_{in'}, Z_x(|\psi\rangle \otimes |\psi'\rangle \otimes |\bar{0}\rangle) = U|\psi\rangle \otimes U^\dagger|\psi'\rangle \otimes |\bar{0}\rangle, \quad (8)$$

$$\rightarrow U_x(|\psi\rangle_{in} \otimes |\bar{0}\rangle_a) \otimes |\psi'\rangle_{in'} = U|\psi\rangle_{in} \otimes U_x(U^\dagger|\psi'\rangle_{in'} \otimes |\bar{0}\rangle_a). \quad (9)$$

From separability, we obtain that

$$U_x(|\psi\rangle \otimes |\bar{0}\rangle) = U|\psi\rangle \otimes |\phi_{\psi,x}\rangle. \quad (10)$$

Thus, all we have to show is that  $|\phi_{\psi,x}\rangle$  does not depend on  $\psi$ . For two different inputs  $|\psi\rangle$  and  $|\psi'\rangle$ ,

$$U_x(|\psi\rangle \otimes |\bar{0}\rangle) = U|\psi\rangle \otimes |\phi_{\psi,x}\rangle, \quad (11)$$

$$U_x(|\psi'\rangle \otimes |\bar{0}\rangle) = U|\psi'\rangle \otimes |\phi_{\psi',x}\rangle. \quad (12)$$

Thus, we easily derive that

$$\langle \psi | \psi' \rangle (1 - \langle \phi_{\psi,x} | \phi_{\psi',x} \rangle) = 0, \quad (13)$$

and we can conclude that  $|\phi_{\psi,x}\rangle$  does not depend on the input. ■

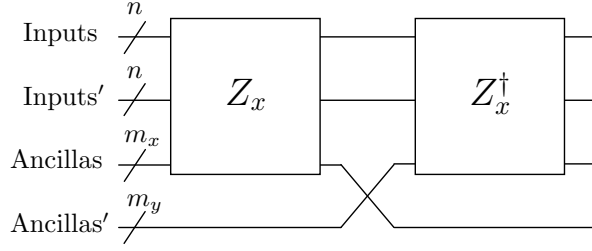


Figure 2: Circuit  $Z_{x,y}$  consisting of  $Z_x$  and  $Z_y^\dagger$ .

From Lemma 2, let us define exact non-identity check problem.

**Definition 5 (Exact non-identity check)**

Let  $x \in \{0,1\}^*$  be a classical description of a quantum circuit  $U_x$  that acts on the Hilbert space  $\mathcal{H}_{in} \otimes \mathcal{H}_a := \mathcal{B}^{\otimes n_x} \otimes \mathcal{B}^{\otimes m_x}$ , where  $n_x$  and  $m_x$  grow at most polynomially in  $|x|$ . Then, decide whether

$$\exists |\Psi\rangle \in \mathcal{H}_{in} \otimes \mathcal{H}_{in'}, \quad |\langle \Psi | \otimes \langle \bar{0} | Z_x(|\Psi\rangle \otimes |\bar{0}\rangle)|^2 \neq 1, \quad (14)$$

$$\text{or } \forall |\Psi\rangle \in \mathcal{H}_{in} \otimes \mathcal{H}_{in'}, \quad |\langle \Psi | \otimes \langle \bar{0} | Z_x(|\Psi\rangle \otimes |\bar{0}\rangle)|^2 = 1. \quad (15)$$

From the definition of exact non-identity check, we give exact equivalence check.

**Definition 6 (Exact equivalence check)**

Let  $x$  and  $y$  be classical descriptions of quantum circuits  $U_x$  and  $U_y$  that act on the Hilbert spaces  $\mathcal{H}_{in} \otimes \mathcal{H}_a := \mathcal{B}^{\otimes n} \otimes \mathcal{B}^{\otimes m_x}$  and  $\mathcal{H}_{in'} \otimes \mathcal{H}_{a'} := \mathcal{B}^{\otimes n} \otimes \mathcal{B}^{\otimes m_y}$ , where  $n$  grow at most polynomially in  $\text{Max}(|x|, |y|)$ . Construct a quantum circuit  $Z_{x,y} = [(Z_x)_{in,in',a} \otimes I_{a'}][(Z_y^\dagger)_{in,in',a'} \otimes I_a]$  in Fig. 2. Then, decide whether

$$\exists |\Psi\rangle \in \mathcal{H}_{in} \otimes \mathcal{H}_{in'}, \quad |\langle \Psi | \otimes \langle \bar{0} | Z_{x,y}(|\Psi\rangle \otimes |\bar{0}\rangle)|^2 \neq 1, \quad (16)$$

$$\text{or } \forall |\Psi\rangle \in \mathcal{H}_{in} \otimes \mathcal{H}_{in'}, \quad |\langle \Psi | \otimes \langle \bar{0} | Z_{x,y}(|\Psi\rangle \otimes |\bar{0}\rangle)|^2 = 1, \quad (17)$$

where  $|\bar{0}\rangle \in \mathcal{H}_a \otimes \mathcal{H}_{a'}$ .

From the definition, exact equivalence check is clearly reducible to exact non-identity check in polynomial time. Let us explain the meaning of “equivalence” in exact equivalence check.

**Lemma 3** Eq.(17) is satisfied if and only if  $U_x$  and  $U_y$  implement an identical unitary operation, i.e., there exists a unitary operation  $U$  such that

$$\forall |\psi\rangle \in \mathcal{H}_{in} (= \mathcal{H}_{in'}), \quad U_i(|\psi\rangle \otimes |\bar{0}\rangle) = U |\psi\rangle \otimes |\phi_i\rangle, \quad (18)$$

for an arbitrary  $i \in \{x, y\}$ .

**Proof** We show the necessary condition, because the sufficient one is derived from direct calculation. If Eq.(17) is satisfied, for an arbitrary  $|\Psi\rangle \in \mathcal{H}_{in} \otimes \mathcal{H}_{in'}$ , we obtain

$$Z_x(|\Psi\rangle \otimes |\bar{0}\rangle_a) \otimes |\bar{0}\rangle_{a'} = Z_y(|\Psi\rangle \otimes |\bar{0}\rangle_{a'}) \otimes |\bar{0}\rangle_a, \quad (19)$$

from which we can derive that  $Z_x$  and  $Z_y$  implement the identical unitary operation  $U$ , i.e.,

$$Z_x(|\Psi\rangle \otimes |\bar{0}\rangle_a) = U|\Psi\rangle \otimes |\bar{0}\rangle_a, \quad (20)$$

$$Z_y(|\Psi\rangle \otimes |\bar{0}\rangle_{a'}) = U|\Psi\rangle \otimes |\bar{0}\rangle_{a'}. \quad (21)$$

Let us show that  $U_x$  implements a unitary operation by contradiction. If  $U_x$  implements no unitary operation, there exists a  $|\psi\rangle \in \mathcal{H}_{in}$  such that

$$U_x(|\psi\rangle \otimes |\bar{0}\rangle_a) = \sum_{i=1}^{d>1} c_i |i\rangle_{in} \otimes |i\rangle_a, \quad (22)$$

where we used Schmidt decomposition and  $c_i$ 's are non-zero coefficients. From Eq.(20), for an orthonormal basis  $\{|k\rangle\}_{k=1}^{\dim \mathcal{H}_{in'}}$  of  $\mathcal{H}_{in'}$ ,

$$\sum_{i=1}^{d>1} c_i |i\rangle_{in} \otimes U_x^\dagger(|k\rangle_{in'} \otimes |i\rangle_a) = \sum_{i=1}^{d>1} c_i |i\rangle_{in} \otimes |\phi_{ki}\rangle_{in'} \otimes |\bar{0}\rangle_a, \quad (23)$$

where  $\langle \phi_{ki} | \phi_{kj} \rangle = \delta_{ij}$ , since local unitary operation does not change entanglement. Further, from linearity, for an arbitrary linear combination  $\alpha |k\rangle_{in'} + \beta |l\rangle_{in'}, (k \neq l)$ ,

$$\begin{aligned} & U_x^\dagger((\alpha |k\rangle_{in'} + \beta |l\rangle_{in'}) \otimes |i\rangle_a) = (\alpha |\phi_{ki}\rangle_{in'} + \beta |\phi_{li}\rangle_{in'}) \otimes |\bar{0}\rangle_a, \\ \rightarrow & \delta_{ij} = |\alpha|^2 \langle \phi_{ki} | \phi_{kj} \rangle + |\beta|^2 \langle \phi_{li} | \phi_{lj} \rangle + \alpha^* \beta \langle \phi_{ki} | \phi_{lj} \rangle + \alpha \beta^* \langle \phi_{li} | \phi_{kj} \rangle, \\ \rightarrow & \langle \phi_{ki} | \phi_{lj} \rangle = \delta_{kl} \delta_{ij}. \end{aligned} \quad (24)$$

Since  $1 \leq k, l \leq \dim \mathcal{H}_{in'}$ ,  $d$  is required to be one, which is the contradiction. ■

## 4 Main Result

Our goal in this paper is to prove the following theorem.

**Theorem 1** Exact non-identity check is NQP-complete.

**Proof** First, let us show that Exact non-identity check is in NQP. For a quantum circuit  $U$  that acts on  $\mathcal{H}_{in} \otimes \mathcal{H}_a = \mathcal{B}^{\otimes n} \otimes \mathcal{B}^{\otimes m}$ , consider the following NQP simulation of exact non-identity check (“verifier”).

- For inputs  $|\bar{0}\rangle \in \mathcal{H}_{in}^{\otimes 3}$ , apply  $H^{\otimes n}$  on the first  $n$  qubits.

- For every  $i \in \{1, \dots, n\}$ , apply controlled-not gates on  $i$ th and  $(n+i)$ th qubit and on  $i$ th and  $(2n+i)$ th qubit. Then, applying  $H^{\otimes n}$  on the last  $n$  qubits, we have input states

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |x\rangle \otimes |x_+\rangle. \quad (25)$$

- Adding ancilla states  $|\bar{0}\rangle \otimes |\bar{0}\rangle \in \mathcal{H}_a \otimes \mathcal{H}_a$  into the state in Eq.(25), apply  $I \otimes U \otimes U$  on the state. As a result, we have the state

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes U(|x\rangle \otimes |\bar{0}\rangle) \otimes U(|x_+\rangle \otimes |\bar{0}\rangle). \quad (26)$$

- Make the measurement on the first  $2n$  inputs in computational basis and on the last  $n$  inputs in  $|x_+\rangle$  basis. Accept if an outcome is not  $(x, x, x)$ .

For the completeness, we use the contradiction. Assume that the verifier never accepts  $U$  though  $U$  implements no identity. Remembering that a probability of an outcome  $(x, y, z)$  is given by

$$\begin{aligned} \Pr(x, y, z) &= \frac{1}{2^n} \langle y | \text{tr}_a [U(|x\rangle \langle x| \otimes |\bar{0}\rangle \langle \bar{0}|) U^\dagger] | y \rangle \\ &\quad \langle z_+ | \text{tr}_a [U(|x_+\rangle \langle x_+| \otimes |\bar{0}\rangle \langle \bar{0}|) U^\dagger] | z_+ \rangle, \end{aligned} \quad (27)$$

we can derive that  $\Pr(x, x, x) = 1/2^n$  from  $\sum_x \Pr(x, x, x) = 1$ . Thus,  $U(|x\rangle \otimes |\bar{0}\rangle)$  and  $U(|x_+\rangle \otimes |\bar{0}\rangle)$  are required to be  $|x\rangle \otimes |\phi_x\rangle$  and  $|x_+\rangle \otimes |\phi'_x\rangle$ . On the other hand, we can calculate directly

$$U(|x_+\rangle \otimes |\bar{0}\rangle) = \frac{1}{\sqrt{2^N}} \sum_y (-1)^{x \cdot y} |y\rangle \otimes |\phi_y\rangle. \quad (28)$$

From the separability, all the  $|\phi_y\rangle$ s must be equal. Thus,  $U$  implements the identity, which contradicts the assumption.

For the soundness, suppose that  $U$  implements the identity. It is trivial that the verifier never accepts  $U$  from the definition of the verifier.

In order to show the NQP-hardness, it is sufficient to show that  $\text{QMA}(\delta, 0)$  is reducible to exact non-identity check, because of Lemma 1. Note that  $\delta : \mathbb{Z}^+ \rightarrow (0, 1]$ . Let  $U$  be a quantum circuit of  $\text{QMA}(\delta, 0)$  generated from  $x \in \{0, 1\}^*$ . From the definition of  $\text{QMA}(\delta, 0)$ , at least  $\delta$  completeness and perfect soundness are satisfied:

$$(\text{Completeness}) \quad \forall x \in L \exists \rho \in \mathcal{S}(\mathcal{B}^{\otimes n_x}), \text{Tr}[U(\rho \otimes |\bar{0}\rangle \langle \bar{0}|) U^\dagger P_1] \geq \delta(|x|), \quad (29)$$

$$(\text{Soundness}) \quad \forall x \notin L \forall \rho \in \mathcal{S}(\mathcal{B}^{\otimes n_x}), \text{Tr}[U(\rho \otimes |\bar{0}\rangle \langle \bar{0}|) U^\dagger P_1] = 0. \quad (30)$$

In order to apply  $U$  to exact non-identity check, we construct a circuit  $Z$  that implements the identity whenever there exists no state accepted by  $U$  or implements no identity if there is a witness. One qubit register is added to extend the inputs and the whole transformation is given

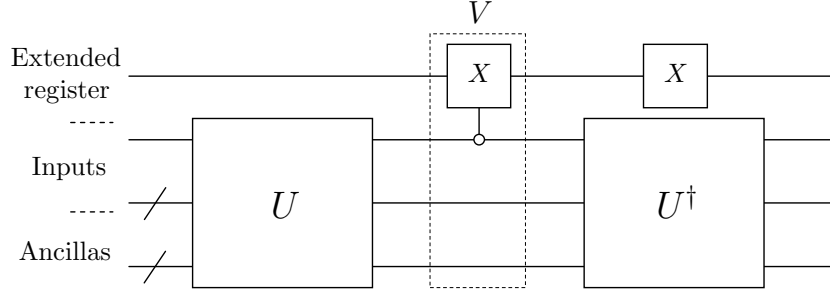


Figure 3: Circuit Z consisting of  $U$ ,  $U^\dagger$ , a controlled- $X$ , and  $X$ . Note that the controlled- $X$  operates when the controlled state is  $|0\rangle$ .

by  $Z := (X \otimes U^\dagger)V(I \otimes U)$ , where  $V$  is a controlled- $X$  which acts on the extended register and is controlled by the first qubit in the original input registers. Note that  $V$  operates when the controlled state is  $|0\rangle$  (See Fig.3). We always set the original ancillas in state  $|\bar{0}\rangle$ .

First, let us show that when Eq.(29) is satisfied,  $Z$  implements no identity. Consider a proof  $|\phi\rangle$ <sup>1</sup> that is accepted by QMA( $\delta, 0$ )-verifier  $U$  with  $\epsilon > 0$  probability, and apply  $Z$  on  $|0\rangle \otimes |\phi\rangle \otimes |\bar{0}\rangle$ . Defining that  $|\Psi\rangle := |0\rangle \otimes U(|\phi\rangle \otimes |\bar{0}\rangle) = \sqrt{1-\epsilon}|0\rangle \otimes |0\rangle \otimes |\Phi\rangle + \sqrt{\epsilon}e^{i\gamma}|0\rangle \otimes |1\rangle \otimes |\Phi'\rangle$ , we calculate that

$$\begin{aligned} Z(|0\rangle \otimes |\phi\rangle \otimes |\bar{0}\rangle) &= (X \otimes U^\dagger)V|\Psi\rangle \\ &= \sqrt{1-\epsilon}|0\rangle \otimes U^\dagger(|0\rangle \otimes |\Phi\rangle) \\ &\quad + \sqrt{\epsilon}e^{i\gamma}|1\rangle \otimes U^\dagger(|1\rangle \otimes |\Phi'\rangle). \end{aligned} \quad (31)$$

Assuming that  $Z$  implements the identity with ancilla,  $Z(|0\rangle \otimes |\phi\rangle \otimes |\bar{0}\rangle)$  must be a separable state in the extended register and the other systems. However, Eq.(31) shows that the state is a bipartite entangled state, which contradicts the assumption. Thus,  $Z$  implements no identity for the input and extended space, *i.e.*,

$$\langle 0| \otimes \langle \phi| \text{tr}_a[Z(|0\rangle \langle 0| \otimes |\phi\rangle \langle \phi| \otimes |\bar{0}\rangle \langle \bar{0}|)Z^\dagger] |0\rangle \otimes |\phi\rangle < 1. \quad (32)$$

Now, we show that  $Z$  implements the identity if there is no witness. It is sufficient to consider arbitrary pure states, since an arbitrary mixed state is rewritten into a probability distribution of orthogonal pure states in the extended and input Hilbert space. Consider a pure state  $|\psi\rangle = \sum_i (c_i |0\rangle \otimes |i\rangle + d_i |1\rangle \otimes |i\rangle)$  in the extended and input Hilbert space, where  $\sum_i (|c_i|^2 + |d_i|^2) =$

<sup>1</sup> Note that there always exists a pure state proof accepted with  $\epsilon > 0$  probability for any mixed state proof accepted with  $\delta$  probability because the mixed state can be written as a probability distribution of orthogonal pure states.



$1, c_i, d_i \in \mathbb{C}$ . Applying  $Z$  on  $|\psi\rangle \otimes |\bar{0}\rangle$ , we derive

$$\begin{aligned}
Z(|\psi\rangle \otimes |\bar{0}\rangle) &= (X \otimes U^\dagger) V \sum_i (c_i |0\rangle \otimes U(|i\rangle \otimes |\bar{0}\rangle) + d_i |1\rangle \otimes U(|i\rangle \otimes |\bar{0}\rangle)) \\
&= (X \otimes U^\dagger) \sum_i (c_i |1\rangle \otimes U(|i\rangle \otimes |\bar{0}\rangle) + d_i |0\rangle \otimes U(|i\rangle \otimes |\bar{0}\rangle)) \\
&= |\psi\rangle \otimes |\bar{0}\rangle,
\end{aligned} \tag{33}$$

where we used the assumption that  $U$  accepts no input state, *i.e.*, Eq.(30). Therefore, we conclude that for an arbitrary quantum state  $|\psi\rangle$ ,

$$\langle\psi| \text{tr}_a[Z(|\psi\rangle \langle\psi| \otimes |\bar{0}\rangle \langle\bar{0}|)Z^\dagger] |\psi\rangle = 1. \tag{34}$$

■

From the NQP-completeness of exact non-identity check, we derive that exact equivalence check is NQP-complete.

**Corollary 1** Exact equivalence check is NQP-complete.

**Proof** Reduction from exact equivalence check to exact non-identity check is trivial. To reduce exact non-identity check to exact equivalence check, for a given  $U_x$ , take  $U_y = I$  in Fig. 2. ■

## 5 Quantum gates minimization problem

As an application of exact non-identity check, we introduce a quantum gates minimization problem of minimizing quantum resources of a quantum gate array without changing the implemented unitary operation, and show that this problem is NQP-hard.

We prepare definitions for quantum gates minimization problem.  $|U_x|$  denotes the number of quantum gates constructing a quantum circuit  $U_x$  generated by a classical inputs  $x \in \{0, 1\}^*$  with respect to fixed universal quantum gates. Define

$$S_U = \{x \in \{0, 1\}^* \mid \exists |\phi_i\rangle \in \mathcal{H}_a \ \forall |\psi\rangle \in \mathcal{H}_{in}, \ U_x(|\psi\rangle \otimes |\bar{0}\rangle) = U |\psi\rangle \otimes |\phi_i\rangle\} \tag{35}$$

as a set of equivalent classical descriptions of an implemented unitary operation  $U$ .

**Definition 7 (Quantum gates minimization problem)**

A classical description  $x$  for a quantum circuit  $U$  is said to be minimized if  $|U_x| = \min_{y \in S_U} |U_y|$ . For a given classical description  $x$ , quantum gates minimization is said to be feasible if a minimized classical description of  $x$  is computed in polynomial-time of  $|x|$ .

So far, we have a corollary from the NQP-completeness of exact non-identity check.

**Corollary 2** Quantum gates minimization problem is NQP-hard.

**Proof** For a given classical description  $x$ , when  $U_x$  implements the identity  $U = I$ ,

$$\min_{y \in S_U} |U_y| = 0. \quad (36)$$

When  $U_x$  implements no identity,  $\min_{y \in S_{U_x}} |U_y| > 0$ . ■

## 6 Summary

We defined exact non-identity check problem of deciding whether a given classical description of a quantum circuit is strictly equivalent to the identity or not, and showed that this problem is NQP-complete. Exact non-identity check is a decision problem of quantum circuits and is useful to analyze quantum gate complexity. For example, as corollaries of our result, we proposed exact equivalence check and quantum gate minimization problem and showed the NQP-completeness and the NQP-hardness respectively.

## 7 Acknowledgements

The author thanks M. Murao, M. Ukita and Y. Kawamoto for useful discussions.

## References

- [1] D. Janzing, P. Wocjan, and T. Beth, *Int. J. Quantum Inf.* **3** (2005) 463.
- [2] L. Adleman, J. DeMarrais, and M. Huang, Quantum computability, *SIAM Journal on Computing* **26** (1997) 1524-1540.
- [3] H. Kobayashi, K. Matsumoto, and T. Yamakami, Quantum Merlin-Arthur Proof Systems: Are Multiple Merlins More Helpful to Arthur?, quant-ph/0306051v2
- [4] A. Y. Kitaev, A. H. Shen, and M. N. Vyalıy, *Classical and Quantum Computation*, Graduate Studies in Mathematics, Vol 47 (American Mathematical Society, 2002).
- [5] S. Fenner, F. Green, S. Homer, and R. Pruim, Determining Acceptance Possibility for a Quantum Computation is Hard for the Polynomial Hierarchy, quant-ph/9812056v1.